Template Version Number: 01-2020

U.S. Department of Commerce
National Oceanic & Atmospheric Administration

Privacy Impact Assessment
for the
NOAA0201
Web Operation Center (WOC)

Reviewed by: Mark H. Graff, Bureau Chief Privacy Officer

☒ Concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer
☐ Non-concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer

Jennifer Goode 01/27/2021

Signature of Senior Agency Official for Privacy/DOC Chief Privacy Officer Date

U.S. Department of Commerce Privacy Impact Assessment
NOAA/OCIO/Web Operation Center

Unique Project Identifier: NOAA0201 (006-48-02-00-01-3511-00)

Introduction: System Description

The WOC is a diverse information technology services provider to Line and Staff Offices within NOAA. The WOC provides a wide range of information technology services and functions which include high availability, scalability, redundancy, clustering, and high performance computing to replicate and distribute general information as well as critical time sensitive life and property information to the general public and meteorology community.

The services and functions of the information system technology have been broken down into four (4) core services and functions: WOC Domain Name System Services (WOCDNSS), WOC Information Sharing Services (WOCISS), WOC Adoptive System Framework (WOCASF), and WOC Collaboration Services (WOCCS). These services and functions make up the subsystems within NOAA0201. Each subsystem has a different FIPS 199 security categorization as described in the NOAA0201 FIPS 199 Security Categorization document.

The WOC systems are physically located at eight (8) NOAA datacenters: (W1: Silver Spring, Maryland; W2: Ashburn, Virginia; W3: Norman, Oklahoma; W4: Boulder, Colorado; W5: Ft. Worth, Texas; W6: Seattle, Washington; W7: Asheville, North Carolina; and W8: Fairmont, West Virginia). As of FY19, the WOC has extended its on premise system boundary to the Amazon Web Services (AWS) platform. AWS is an on-demand cloud computing platform extending the WOC into AWS US-East Region (Northern Virginia).

Provide a description of the system that addresses the following elements:
The response must be written in plain language and be as comprehensive as necessary to describe the system.

(a) Whether it is a general support system, major application, or other type of system

NOAA0201 WOC is a General Support System (GSS).

(b) System location

NOAA0201 WOC has information system equipment located in multiple federal datacenters for the purpose of redundancy and fault tolerance:

W1 - NOAA0201 – NOAA HQS Silver Spring Metro Center 3 (SSMC3) - Silver Spring, MD
W2 - NOAA0520 – NOAA Enterprise Data Centers (NEDC) - Ashburn VA
W3 - NOAA3090 – NSSL - Norman, OK
W4 - NOAA3400 – BNOC - Boulder, CO
W5 - NOAA8884 – SRHQ - Fort Worth, TX
W6 - NOAA3100 – PMELLAN - Seattle, WA
W7 - NOAA5009 – NCDC - Ashville, NC
W8 - NOAA0520 – NESCC - Fairmont, WV

(c) Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects)

NOAA0201 is not a standalone system and interconnects with the following NOAA information systems:
NOAA1101 - Information Technology Center
NOAA3090 - National Severe Storms Laboratory Scientific Computing Facility
NOAA5009 - National Climatic Data Center Local Area Network
NOAA5040 - Comprehensive Large Array-data Stewardship System
NOAA8860 - Weather and Climate Computing Infrastructure Services (WCCIS)
NOAA8868 - Storm Prediction Center
NOAA8873 - National Data Buoy Center
NOAA8884 - SR Fort Worth
NOTE: There is no sharing of information with any system other than NOAA1101. The other connections only utilize the web tools from NOAA0201.

(d) The way the system operates to achieve the purpose(s) identified in Section 4

NOAA0201 WOC provides data-dissemination business processes to distribute scientific and meteorological data, general information, and critical time sensitive life and property information to the public and meteorology community. This data is processed by other NOAA information systems and other federal agencies for use by the federal government and the public.

These purposes are achieved by NOAA0201's four (4) core services and functions: WOC Domain Name System Services (WOCDNSS), WOC Information Sharing Services (WOCISS), WOC Adoptive System Framework (WOCASF), and WOC Collaboration Services (WOCCS). These services and functions make up the subsystems within NOAA0201. Each subsystem has a different FIPS 199 security categorization as described in the NOAA0201 FIPS 199 Security Categorization document.

(e) How information in the system is retrieved by the user

Only NOAA personnel (government employees and/or contractors) with valid user accounts and

authentication may access information in the system. Access requires the use of GFE. Remote access requires the use of VPN.

(f) How information is transmitted to and from the system

All data is encrypted in transit.

(g) Any information sharing conducted by the system

NOAA0201 WOC provides data-dissemination business processes to distribute scientific and meteorological data and information gathered from a variety of sources across the globe. This data is processed by other NOAA information systems and other federal agencies for general use by the federal government and the public. In addition to the scientific and meteorological data, NOAA0201 contains PII in the form of contractor and federal employee contact information (name, phone number(s), email address(es), user ID) gathered from the employee(s) during the hiring process via phone and email. The information is vetted during the hiring and badging processes and used for administrative purposes only.

(h) The specific programmatic authorities (statutes or Executive Orders) for collecting, maintaining, using, and disseminating the information

This system is covered by an existing system of records notice COMMERCE/DEPT-18

(i) The Federal Information Processing Standards (FIPS) 199 security impact category for the system

The FIPS 199 Security Categorization for NOAA0201 WOC is High (CIA = L, H, H).

Section 1: Status of the Information System

1.1 Indicate whether the information system is a new or existing system.

_____ This is a new information system.
_____ This is an existing information system with changes that create new privacy risks. *(Check all that apply.)*

Changes That Create New Privacy Risks (CTCNPR)					
a. Conversions		d. Significant Merging		g. New Interagency Uses	
b. Anonymous to Non-Anonymous		e. New Public Access		h. Internal Flow or Collection	
c. Significant System Management Changes		f. Commercial Sources		i. Alteration in Character of Data	
j. Other changes that create new privacy risks (specify):					

____ This is an existing information system in which changes do not create new privacy risks, and there is not a SAOP approved Privacy Impact Assessment.

X This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment (version 01-2015 or 01-2017).

____ This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment (version 01-2019 or later).

Section 2: Information in the System

2.1 Indicate what personally identifiable information (PII)/business identifiable information (BII) is collected, maintained, or disseminated. *(Check all that apply.)*

Identifying Numbers (IN)					
a. Social Security*		f. Driver's License		j. Financial Account	
b. Taxpayer ID		g. Passport		k. Financial Transaction	
c Employer ID		h. Alien Registration		l. Vehicle Identifier	
d. Employee ID		i. Credit Card		m Medical Record	
e. File/Case ID					
n. Other identifying numbers (specify):					
*Explanation for the business need to collect, maintain, or disseminate the Social Security number, including truncated form:					

General Personal Data (GPD)					
a. Name	X	h. Date of Birth		o. Financial Information	

b. Maiden Name		i. Place of Birth		p. Medical Information	
c. Alias		j. Home Address		q. Military Service	
d. Gender		k. Telephone Number		r. Criminal Record	
e. Age		l. Email Address		s. Physical Characteristics	
f. Race/Ethnicity		m. Education		t. Mother's Maiden Name	
g. Citizenship		n. Religion			
u. Other general personal data (specify):					

Work-Related Data (WRD)					
a. Occupation		e. Work Email Address	X	i. Business Associates	
b. Job Title		f. Salary		j. Proprietary or Business Information	
c. Work Address	X	g. Work History		k. Procurement/contracting records	
d. Work Telephone Number	X	h. Employment Performance Ratings or other Performance Information			
l. Other work-related data (specify):					

Distinguishing Features/Biometrics (DFB)					
a. Fingerprints		f. Scars, Marks, Tattoos		k. Signatures	
b. Palm Prints		g. Hair Color		l. Vascular Scans	
c. Voice/Audio Recording		h. Eye Color		m. DNA Sample or Profile	
d. Video Recording		i. Height		n. Retina/Iris Scans	
e. Photographs		j. Weight		o. Dental Profile	
p. Other distinguishing features/biometrics (specify):					

System Administration/Audit Data (SAAD)					
a. User ID	X	c. Date/Time of Access		e. ID Files Accessed	
b. IP Address		f. Queries Run		f. Contents of Files	
g. Other system administration/audit data (specify):					

Other Information (specify)

2.2 Indicate sources of the PII/BII in the system. *(Check all that apply.)*

Directly from Individual about Whom the Information Pertains					
In Person	X	Hard Copy: Mail/Fax		Online	
Telephone		Email	X		
Other (specify):					

Government Sources					
Within the Bureau		Other DOC Bureaus		Other Federal Agencies	
State, Local, Tribal		Foreign			

Other (specify):

Non-government Sources					
Public Organizations		Private Sector		Commercial Data Brokers	
Third Party Website or Application					
Other (specify):					

2.3 Describe how the accuracy of the information in the system is ensured.

The information pertains to DOC and contractor employees. The accuracy of the information is vetted during the hiring and security badging processes.

2.4 Is the information covered by the Paperwork Reduction Act?

	Yes, the information is covered by the Paperwork Reduction Act. Provide the OMB control number and the agency number for the collection.
X	No, the information is not covered by the Paperwork Reduction Act.

2.5 Indicate the technologies used that contain PII/BII in ways that have not been previously deployed. *(Check all that apply.)*

Technologies Used Containing PII/BII Not Previously Deployed (TUCPBNPD)			
Smart Cards		Biometrics	
Caller-ID		Personal Identity Verification (PIV) Cards	
Other (specify):			

X	There are not any technologies used that contain PII/BII in ways that have not been previously deployed.

Section 3: System Supported Activities

3.1 Indicate IT system supported activities which raise privacy risks/concerns. *(Check all that apply.)*

Activities			
Audio recordings		Building entry readers	
Video surveillance		Electronic purchase transactions	
Other (specify):			

X	There are not any IT system supported activities which raise privacy risks/concerns.

Section 4: Purpose of the System

4.1 Indicate why the PII/BII in the IT system is being collected, maintained, or disseminated. *(Check all that apply.)*

Purpose			
For a Computer Matching Program		For administering human resources programs	
For administrative matters	X	To promote information sharing initiatives	
For litigation		For criminal law enforcement activities	
For civil enforcement activities		For intelligence activities	
To improve Federal services online		For employee or customer satisfaction	
For web measurement and customization technologies (single-session)		For web measurement and customization technologies (multi-session)	
Other (specify):			

Section 5: Use of the Information

5.1 In the context of functional areas (business processes, missions, operations, etc.) supported by the IT system, describe how the PII/BII that is collected, maintained, or disseminated will be used. Indicate if the PII/BII identified in Section 2.1 of this document is in reference to a federal employee/contractor, member of the public, foreign national, visitor or other (specify).

The information which is subject to this PIA is not private and is not sensitive. The information is used for IT administration and for identity verification (federal employees and contractors).

5.2 Describe any potential threats to privacy, such as insider threat, as a result of the bureau's/operating unit's use of the information, and controls that the bureau/operating unit has put into place to ensure that the information is handled, retained, and disposed appropriately. (For example: mandatory training for system users regarding appropriate handling of information, automatic purging of information in accordance with the retention schedule, etc.)

Potential threats include the potential for unintentional disclosure of PII. This threat is countered by training all personnel with respect to cyber security, privacy, and awareness training annually. The information is retained in accordance with departmental policies.

Section 6: Information Sharing and Access

6.1 Indicate with whom the bureau intends to share the PII/BII in the IT system and how the PII/BII will be shared. *(Check all that apply.)*

Recipient	How Information will be Shared		
	Case-by-Case	Bulk Transfer	Direct Access
Within the bureau	X		
DOC bureaus			
Federal agencies			
State, local, tribal gov't agencies			
Public			
Private sector			
Foreign governments			
Foreign entities			
Other (specify):			

	The PII/BII in the system will not be shared.

6.2 Does the DOC bureau/operating unit place a limitation on re-dissemination of PII/BII shared with external agencies/entities?

	Yes, the external agency/entity is required to verify with the DOC bureau/operating unit before re-dissemination of PII/BII.
	No, the external agency/entity is not required to verify with the DOC bureau/operating unit before re-dissemination of PII/BII.
X	No, the bureau/operating unit does not share PII/BII with external agencies/entities.

6.3 Indicate whether the IT system connects with or receives information from any other IT systems authorized to process PII and/or BII.

X	Yes, this IT system connects with or receives information from another IT system(s) authorized to process PII and/or BII. Provide the name of the IT system and describe the technical controls which prevent PII/BII leakage: Interconnected System: NOAA1101 GSS The information is used for IT administration and for identity verification (federal employees and contractors). The information is encrypted while at rest and while in transit. All staff receive annual cyber security, privacy, and awareness training. The PII/BII information contained in each system is not shared between the systems. NOAA0201 does not share PII/BII with any other system.
	No, this IT system does not connect with or receive information from another IT system(s) authorized to process PII and/or BII.

6.4 Identify the class of users who will have access to the IT system and the PII/BII. *(Check all that apply.)*

Class of Users			
General Public		Government Employees	X
Contractors	X		
Other (specify):			

Section 7: Notice and Consent

7.1 Indicate whether individuals will be notified if their PII/BII is collected, maintained, or disseminated by the system. *(Check all that apply.)*

X	Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 9.	
	Yes, notice is provided by a Privacy Act statement and/or privacy policy. The Privacy Act statement and/or privacy policy can be found at: .	
X	Yes, notice is provided by other means.	Specify how: Notice is provided as part of employee enrollment, and on the staff directory warning banner.
	No, notice is not provided.	Specify why not:

7.2 Indicate whether and how individuals have an opportunity to decline to provide PII/BII.

X	Yes, individuals have an opportunity to decline to provide PII/BII.	Specify how: An individual may decline but would not have access to the NOAA IT network.
	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not:

7.3 Indicate whether and how individuals have an opportunity to consent to particular uses of their PII/BII.

X	Yes, individuals have an opportunity to consent to particular uses of their PII/BII.	Specify how: There is only one use, which is explained during employee orientation.
	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not:

7.4 Indicate whether and how individuals have an opportunity to review/update PII/BII pertaining to them.

X	Yes, individuals have an opportunity to review/update PII/BII pertaining to them.	Specify how: Individuals may view their info online and make a request for a change.

	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not:

Section 8: Administrative and Technological Controls

8.1 Indicate the administrative and technological controls for the system. *(Check all that apply.)*

X	All users signed a confidentiality agreement or non-disclosure agreement.
X	All users are subject to a Code of Conduct that includes the requirement for confidentiality.
X	Staff (employees and contractors) received training on privacy and confidentiality policies and practices.
X	Access to the PII/BII is restricted to authorized personnel only.
	Access to the PII/BII is being monitored, tracked, or recorded. Explanation:
X	The information is secured in accordance with the Federal Information Security Modernization Act (FISMA) requirements. Provide date of most recent Assessment and Authorization (A&A): July 7, 2020 ☐ This is a new system. The A&A date will be provided when the A&A package is approved.
X	The Federal Information Processing Standard (FIPS) 199 security impact category for this system is a moderate or higher.
X	NIST Special Publication (SP) 800-122 and NIST SP 800-53 Revision 4 Appendix J recommended security controls for protecting PII/BII are in place and functioning as intended; or have an approved Plan of Action and Milestones (POA&M).
X	A security assessment report has been reviewed for the information system and it has been determined that there are no additional privacy risks.
X	Contractors that have access to the system are subject to information security provisions in their contracts required by DOC policy.
	Contracts with customers establish DOC ownership rights over data including PII/BII.
	Acceptance of liability for exposure of PII/BII is clearly defined in agreements with customers.
	Other (specify):

8.2 Provide a general description of the technologies used to protect PII/BII on the IT system. *(Include data encryption in transit and/or at rest, if applicable).*

NOAA0201 uses audit logging and multi-factor authentication to protect the PII/BII in the system. Only NOAA personnel with authenticated access would be able to change or delete information.

Section 9: Privacy Act

9.1 Is the PII/BII searchable by a personal identifier (e.g., name or Social Security number)?

X Yes, the PII/BII is searchable by a personal identifier.

____ No, the PII/BII is not searchable by a personal identifier.

9.2 Indicate whether a system of records is being created under the Privacy Act, 5 U.S.C. § 552a. *(A new system of records notice (SORN) is required if the system is not covered by an existing SORN).*
As per the Privacy Act of 1974, "the term 'system of records' means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual."

X	Yes, this system is covered by an existing system of records notice (SORN). Provide the SORN name, number, and link. *(list all that apply)*: COMMERCE/DEPT-18
	Yes, a SORN has been submitted to the Department for approval on (date).
	No, this system is not a system of records and a SORN is not applicable.

Section 10: Retention of Information

10.1 Indicate whether these records are covered by an approved records control schedule and monitored for compliance. *(Check all that apply.)*

X	There is an approved record control schedule. Provide the name of the record control schedule: NOAA Records Disposition Handbook Chapter 200-12
	No, there is not an approved record control schedule. Provide the stage in which the project is in developing and submitting a records control schedule:
X	Yes, retention is monitored for compliance to the schedule.
	No, retention is not monitored for compliance to the schedule. Provide explanation:

10.2 Indicate the disposal method of the PII/BII. *(Check all that apply.)*

Disposal			
Shredding		Overwriting	
Degaussing		Deleting	X
Other (specify):			

Section 11: NIST Special Publication 800-122 PII Confidentiality Impact Level

11.1 Indicate the potential impact that could result to the subject individuals and/or the organization if PII were inappropriately accessed, used, or disclosed. *(The PII Confidentiality Impact Level is not the same, and does not have to be the same, as the*

Federal Information Processing Standards (FIPS) 199 security impact category.)

X	**Low –** the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.
	Moderate – the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
	High – the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

11.2 Indicate which factors were used to determine the above PII confidentiality impact level. *(Check all that apply.)*

X	Identifiability	Provide explanation: Minimal admin information for IT work identity.
X	Quantity of PII	Provide explanation: Minimal work contact information.
X	Data Field Sensitivity	Provide explanation: There are no sensitive data fields.
X	Context of Use	Provide explanation: Minimal data for IT user identification.
	Obligation to Protect Confidentiality	Provide explanation:
	Access to and Location of PII	Provide explanation:
	Other:	Provide explanation:

Section 12: Analysis

12.1 Identify and evaluate any potential threats to privacy that exist in light of the information collected or the sources from which the information is collected. Also, describe the choices that the bureau/operating unit made with regard to the type or quantity of information collected and the sources providing the information in order to prevent or mitigate threats to privacy. (For example: If a decision was made to collect less data, include a discussion of this decision; if it is necessary to obtain information from sources other than the individual, explain why.)

The potential threats associated with the gathering of this information is thought to be minimal. The information collected from federal and contractor employees is for administrative purposes only, and is collected during hiring and badging processes. The information is retained in accordance with departmental policies and all staff are trained with respect to cyber security and privacy concerns on an annual basis.

12.2 Indicate whether the conduct of this PIA results in any required business process changes.

	Yes, the conduct of this PIA results in required business process changes. Explanation:
X	No, the conduct of this PIA does not result in any required business process changes.

12.3 Indicate whether the conduct of this PIA results in any required technology changes.

	Yes, the conduct of this PIA results in required technology changes. Explanation:
X	No, the conduct of this PIA does not result in any required technology changes.